VIII kadencja

SEJM RZECZYPOSPOLITEJ POLSKIEJ

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 37)**

z dnia 19 października 2016 r.

Pełny zapis przebiegu posiedzenia

Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 37)

19 października 2016 r.

Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, obradująca pod przewodnictwem posła **Pawła Pudłowskiego (N)**, przewodniczącego Komisji, rozpatrzyła:

– informację Ministra Cyfryzacji o Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020,

– informację Ministra Cyfryzacji o pracach nad rządowym projektem ustawy o krajowym systemie cyberbezpieczeństwa, będącej również transpozycją dyrektywy NIS.

W posiedzeniu udział wzięli: **Anna Streżyńska** minister cyfryzacji wraz ze współpracownikami, płk **Paweł Dziuba** radca ds. cyberprzestrzeni w pionie podsekretarza stanu Ministerstwa Obrony Narodowej, **Mariusz Kujawski** starszy specjalista w Departamencie Teleinformatyki Ministerstwa Spraw Wewnętrznych i Administracji, kpt. **Piotr Burczaniuk** p.o. zastępcy dyrektora Biura Prawnego Agencji Bezpieczeństwa Wewnętrznego, **Bogusław Cichoń** dyrektor Departamentu Prawa i Bezpieczeństwa Pozamilitarnego Biura Bezpieczeństwa Narodowego wraz ze współpracownikami, **Marlena Niewiadomska** zastępca naczelnika CERT.GOV.PL, **Tomasz Sordyl** wicedyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli, **Tomasz Mikołajewski** dyrektor Narodowego Centrum Kryptologii, **Robert Tyszkiewicz** specjalista zajmujący samodzielne stanowisko ds. obsługi legislacyjnej Rządowego Centrum Bezpieczeństwa, **Borys Iwaszko** dyrektor Biura Bezpieczeństwa Cybernetycznego Służby Kontrwywiadu Wojskowego, **Marek Jurkiewicz** naczelnik Wydziału Spraw Obronnych Departamentu Bezpieczeństwa Telekomunikacyjnego Urzędu Komunikacji Elektronicznej wraz ze współpracownikiem, **Wiesław Paluszyński** wiceprezes Polskiej Izby Informatyki i Telekomunikacji, **Marian Noga** prezes Polskiego Towarzystwa Informatycznego, **Bartłomiej Szymczak** ekspert Zespołu ds. cyberbezpieczeństwa Polskiego Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej oraz **Michał Kanownik** prezes zarządu ZIPSEE „Cyfrowa Polska".

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Ewa Gast**, **Julia Popławska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Paweł Pudłowski (N):

Szanowni państwo. Otwieram posiedzenie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii. Witam serdecznie wszystkich państwa. Stwierdzam kworum.

Stwierdzam przyjęcie protokołów z posiedzeń Komisji od nr 2. do 29. wobec niewniesienia do nich zastrzeżeń.

Przechodzimy do przedstawienia i przyjęcia porządku dziennego. Porządek dzisiejszego posiedzenia zawiera rozpatrzenie informacji ministra cyfryzacji o pracach nad rządowym projektem ustawy o krajowym systemie cyberbezpieczeństwa, będącej również transpozycją dyrektywy NIS, oraz rozpatrzenie informacji ministra cyfryzacji o strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020.

Powyższy porządek i materiał członkowie Komisji otrzymali. Czy są uwagi do porządku dziennego?

Ja mam jedną uwagę. Jeżeli nikt nie miałby nic przeciwko temu, to odwrócilibyśmy porządek obrad. Najpierw rozpatrzylibyśmy strategię, a później wynikającą ze strategii

ustawę. Czy tak możemy się umówić? Dziękuję bardzo. Stwierdzam, że Komisja przyjęła porządek dzienny bez zmian, ale ze zmienioną kolejnością.

Zanim przystąpimy do realizacji porządku dziennego, proponuję łącznie rozpatrzyć oba punkty, ale w takiej kolejności, w jakiej uzgodniliśmy.

Przystępujemy do realizacji porządku dziennego. Bardzo proszę panią minister o przedstawienie informacji.

Minister cyfryzacji Anna Streżyńska:

Panie przewodniczący, Wysoka Komisjo. Widzieliśmy się na posiedzeniu Komisji prawie równo rok temu, na pierwszym spotkaniu ministra cyfryzacji z Komisją Cyfryzacji, Innowacyjności i Nowoczesnych Technologii. Wtedy jednym z tematów, które wymagały dużej, wytężonej pracy, było właśnie cyberbezpieczeństwo. Ta kwestia została podsumowana raportem Najwyższej Izby Kontroli w 2015 r., a następnie, na początku 2016 r., jeszcze jednym raportem częściowym, dotyczącym bezpieczeństwa rejestrów i systemów baz danych. Raporty NIK pokazywały, że jest bardzo dużo do zrobienia w tej dziedzinie, nie tylko w ówczesnym Ministerstwie Administracji i Cyfryzacji, potem już Ministerstwie Cyfryzacji – tj. organie koordynującym zagadnienia cyberbezpieczeństwa zgodnie z ustawą o działach administracji rządowej – ale praktycznie w całej przestrzeni administracji publicznej, państwowej i samorządowej.

Dzisiaj jesteśmy już po wykonaniu szeregu różnych działań faktycznych i dokumentacyjnych, które tworzą bazę systemu ochrony cyberbezpieczeństwa w kraju. Te prace odnoszą się przede wszystkim do sektora cywilnego, administracji i biznesu. Starają się wykorzystać to, co w cyberbezpieczeństwie jest zarazem najcenniejsze, jak i nieodzowne, czyli synergię działań różnych interesariuszy, współpracę mającą na celu zapewnienie właściwego przepływu informacji i w efekcie zwiększenia poziomu świadomości, szybkość reagowania i zakreślenie wspólnych ram systemu cyberbezpieczeństwa.

Mamy dzisiaj w planie przedstawienie państwu dwóch prezentacji.

Pierwsza będzie dotyczyła informacji na temat strategii – zarówno jej treści, jak i przebiegu prac i dalszych planów z nią związanych. W tej kwestii jesteśmy w tej chwili pod koniec uzgodnień międzyresortowych.

Tak więc jeśli pan przewodniczący pozwoli, to uruchomimy prezentację i oddam głos kolegom.

Przewodniczący poseł Paweł Pudłowski (N):

Proszę bardzo.

Dyrektor Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji gen. Włodzimierz Nowak:

Panie przewodniczący, Wysoka Komisjo. Włodzimierz Nowak. Departament Cyberbezpieczeństwa MC. Mam zaszczyt przedstawić państwu informację na temat planu pracy i głównych założeń strategii cyberbezpieczeństwa.

Szanowni państwo, co wchodzi w skład strategii cyberbezpieczeństwa? Przede wszystkim realizacja najpilniejszych zadań wynikających z kolejnych raportów NIK, dotyczących stanu rejestrów państwowych, stanu zabezpieczenia naszych systemów teleinformatycznych. Niestety, w efekcie wieloletnich zaniedbań skala problemu jest na tyle wysoka, że MC musiało napisać do pani premier niejawną notatkę opisującą stan faktyczny rejestrów, m.in. w jaki sposób są zabezpieczone, a raczej w jaki sposób nie są zabezpieczone.

Stąd też strategia pełni parę funkcji. Po pierwsze, realizuje najpilniejsze zadania związane ze stanem aktualnym. Po drugie, stanowi wypełnienie uregulowań dyrektywy NIS, czyli wszystkich zaleceń, które wskazała Unia Europejska dla systemów teleinformatycznych, jak również przygotowanie do nowych wyzwań, takich jak IPv6, Internet rzeczy, *smart city*, *smart industry* i inne technologie, które wejdą na rynek w najbliższym czasie.

To jest o tyle istotne, że implementacja wymienionych technologii w najbliższym okresie, czyli do roku 2020, zwiększy ponad czterokrotnie liczbę komputerów włączonych do sieci. Z dzisiejszych 6,4 miliarda na świecie wzrośnie do 21 miliardów. Niektóre

statystyki podają nawet, że nastąpi zwiększenie liczby komputerów do 30 miliardów. Oczywiście, to proporcjonalnie przekłada się na to, co będzie się działo w Polsce.

Nasze podejście do funkcji bezpieczeństwa w cyberprzestrzeni wynika ze szkolnego modelu OSI, który od warstwy sieciowej do warstwy aplikacji opisuje wszystkie urządzenia i elementy systemu teleinformatycznego i komputerowego. Dlaczego jest to takie ważne? Dlatego że inwestowanie tylko w górne warstwy aplikacji, czy sesji przetwarzania danych, byłoby zupełnie nieuzasadnione, ponieważ efekt mógłby być dokładnie taki sam, jeśli zostałyby przerwane te warstwy najniższe, ponieważ dzisiaj urządzenia teletransmisyjne radiolinii też posiadają oprogramowanie. Też są zarządzane poprzez sieć komputerową, też podlegają atakom cybernetycznym.

Naszym zadaniem jest ochrona istotnych funkcji państwa, czyli zadań, które państwo będzie realizowało przy pomocy systemów informatycznych: usługi bankowe, dostęp do rejestrów państwowych, sterowanie miastami, sterowanie transportem. Utrata komunikacji pomiędzy tymi systemami daje dokładnie taki sam efekt, jak zaatakowanie samego systemu sterowania, czyli te funkcje nie są po prostu wypełniane.

Trzy dolne warstwy stanowią głównie infrastrukturę krytyczną, która pozostaje co do zasady w gestii Rządowego Centrum Bezpieczeństwa, natomiast my przyglądamy się tej infrastrukturze pod kątem zabezpieczenia systemów teleinformatycznych, które są tam wykorzystywane, ich oprogramowaniu, sterowaniu oraz serwisowaniu. Na dole slajdu widnieje flagowe zdanie bezpieczników: „łańcuch bezpieczeństwa jest tak mocny, jak jego najsłabsze ogniowo”. Stąd też każde z ogniw jest niezmiernie istotne i jednakowo ważne w systemie.

Plany w zakresie cyberbezpieczeństwa i nasza strategia opierają się na paru filarach. Są to: ludzie, technologie i procedury.

Filar ludzki omówię trochę później, bo jest to cały proces szkolenia różnych grup zawodowych, jak i wszystkich obywateli.

Technologie są w większości dostępne na rynku, częściowo produkowane przez polskie firmy. W zależności od zagrożenia, jakie napotykamy, powinny być stosowane odpowiednie technologie. Przede wszystkim powinny być one bezpieczne.

Przechodzę do procedur. Z procedurami poradziliśmy sobie w ten sposób, że 4 lipca zostało powołane Narodowe Centrum Cyberbezpieczeństwa, które uporządkowało sprawy wymiany informacji pomiędzy służbami państwowymi, najważniejszymi sektorami w państwie, jak również komunikację w kierunku operatorów telekomunikacyjnych.

Ze względu na szybki postęp technologiczny niezmiernie ważną rzeczą są prace badawczo-rozwojowe. Ten obszar też jest uwypuklony w strategii, ponieważ zlecanie prac nie może być procesem długofalowym na pięć, siedem lat. Proces musi być o wiele krótszy, ponieważ technologie w przeciągu dwóch, trzech, czterech lat diametralnie się zmieniają. Stąd też prace badawczo-rozwojowe muszą być prowadzone dynamicznie, mniejszymi zadaniami, ale wykonywanymi szybciej.

Współpraca międzynarodowa to jest kolejny obszar, który jest strategiczny w działaniu w cyberprzestrzeni, ponieważ jeśli nawet jesteśmy geograficznie daleko od jakiegoś kraju, to w cyberprzestrzeni możemy być sąsiadami. Możemy sąsiadować poprzez transgraniczne punkty wymiany Internetu. Dlatego współpraca międzynarodowa musi być ścisła ze wszystkimi krajami regionu i tymi krajami, z którymi mamy bezpośrednie połączenia telekomunikacyjne.

Najistotniejsza sprawa jak zawsze na końcu. Finansowanie przewidujemy częściowo z budżetu państwa, częściowo z funduszy samorządów terytorialnych, jak również z partnerstwa publiczno-prywatnego. Rysuje się również szansa finansowania pewnych rzeczy z funduszy europejskich.

Jakie podejmujemy działania w zakresie architektury systemu bezpieczeństwa i jakie chcemy podjąć? Chcemy zorganizować trzypoziomowy system ochrony krajowej cyberprzestrzeni. Po pierwsze, system wczesnego ostrzegania. Po drugie, klastry bezpieczeństwa – w tym jeden rządowy. Po trzecie, bezpośrednia ochrona danych. Ten system za chwilę omówię.

Po pierwsze, system wczesnego ostrzegania. Ma to być narzędzie, którym będzie posługiwało się Narodowe Centrum Bezpieczeństwa zbierając dane z tzw. transgranicz-

nych punktów wymiany Internetu. Cyberprzestrzeń granic nie ma, natomiast Internet ma granice. Jego granicami są transgraniczne punkty wymiany. Operatorzy telekomunikacyjni monitorują te punkty, natomiast nikt nie agreguje danych od kilku operatorów. Natomiast dzisiaj ataki cybernetyczne polegają na tym, że atakuje się kraj wieloma drogami, przez wielu operatorów. Stąd też zebranie tych samych parametrów od różnych operatorów może nam wskazać wektor ataku. Może nam wskazać konkretne zagrożenie, konkretny rejon, z którego przychodzi atak na określony sektor w naszym państwie. A jak wiemy, skąd ten atak przychodzi, to możemy go zablokować na transgranicznych punktach wymiany Internetu.

Dlaczego jest to możliwe właśnie w Polsce? Spójrzmy na hiperboliczną mapę Internetu. Zobaczmy, jak Polska jest usytuowana w systemie połączeń na poziomie trzecim i drugim. Przepraszam, może linie są trochę niedokładnie widoczne, ale jeżeli ktoś jest zainteresowany, to może sobie obejrzeć tę mapę w Internecie.

Widać, że Polska jest jakby wyizolowana. Oznacza to, że mamy ograniczoną, policzalną liczbę połączeń transgranicznych na poziomie trzecim i drugim, co daje nam możliwość ochrony terytorium naszego państwa. Właśnie w ten sposób, poprzez monitorowanie punktów transgranicznych. Nie jest to możliwe w przypadku Estonii i Gruzji, które są praktycznie wtopione w system rosyjski.

Klastry bezpieczeństwa, to jest dodatkowa ochrona przewidziana w szczególności dla klastra rządowego. Dodatkowa ochrona rejestrów państwowych i serwisów urzędów państwowych. Polega to na zbudowaniu Intranetu, który będzie dodatkowo na wejściu filtrował tzw. spam. Będzie mógł blokować niepożądane oprogramowanie. Będzie dawał możliwość administrowania systemami państwowymi nie wychodząc do otwartego Internetu. Dzisiaj odbywa się to poprzez normalny, otwarty Internet. Administratorzy kontentu zmieniają treści, które są przekazywane społeczeństwu przez rząd. W przyszłości będzie się to odbywało w sieci quasi zamkniętej. Zwiększy to również bezpieczeństwo dostępu do wspomnianych zasobów.

Podobne klastry bezpieczeństwa planujemy na poziomie regionalnym. Muszę wskazać, że jest jedno miasto, które wyszło przed szereg i samo wprowadziło te rozwiązania. Tym miastem jest Ełk. Zbudowano miejski klaster bezpieczeństwa, do którego podłączono wszystkie urzędy administracji samorządowej. Zatrudniono dwóch informatyków, którzy to nadzorują. Tym sposobem miasto zorganizowało swój miejski klaster.

Idea klastra regionalnego jest taka, żeby nie każdy urząd, gmina, powiat zatrudniał informatyków – bo oni i tak będą pracowali od 8 do 16. Po to chcemy zbudować *security operations center* w jednym miejscu, np. w województwie, które to centrum będzie obsługiwało wszystkie urzędy gminne, powiatowe i inne, które będą chciały być zabezpieczane przez taki klaster. Jedynym kosztem, który poniesie samorząd, będzie utrzymanie ludzi w tym centrum. Jednakże, biorąc pod uwagę możliwość składkowego utrzymania, będzie to o wiele tańsze, niż indywidualne zatrudnianie.

Omawiana przeze mnie kwestia jest również bardzo ważna. Niestety w naszym kraju wiele systemów, i to bardzo ważnych, było zbudowanych i jest zbudowanych w ten sposób, że jest system główny, *backup*, archiwum oraz kopia zapasowa, która jest albo jej nie ma. Te wszystkie elementy znajdują się bardzo często w jednym miejscu, w jednym pomieszczeniu albo w jednym budynku. Takie rozwiązanie nie gwarantuje bezpieczeństwa danych. Dlatego chcemy wprowadzić zasadę, by część archiwum i kopia zapasowa była oddalone od miejsca dyslokacji głównego centrum danych. To musi być ok. 70–100 km, aby to było efektywne, aby efektywnie można było replikować dane.

Całościowo system krajowy będzie wyglądał w następujący sposób: system wczesnego ostrzegania, monitorowania punktów transgranicznych, wewnątrz klastry bezpieczeństwa, dodatkowo filtrujące niepożądane oprogramowanie i bezpośrednia ochrona danych polegająca na umiejscowieniu archiwów i kopii zapasowych w innych miejscach niż bazy danych, które będą eksploatowane.

Organizacja systemu wymaga współpracy najważniejszych graczy, jeżeli chodzi o cyberbezpieczeństwo: resortu obrony narodowej, spraw wewnętrznych i Agencji Bezpieczeństwa Wewnętrznego. Wymienione podmioty, zgodnie z naszą strategią, zachowują wszystkie swoje kompetencje, ponieważ są one niezależne od siebie.

Ministerstwo Obrony Narodowej jest wiodące w zakresie obrony kraju, przygotowania planów operacyjnych, jak również zdolności ofensywnych. Ministerstwo Spraw Wewnętrznych i Administracji, razem z policją, jest wiodące w przypadkach pospolitych przestępstw, pornografii w sieci, oszustw finansowych. Natomiast ABW zajmuje się obszarem monitorowania istotnych funkcji państwa, czyli monitorowaniem infrastruktury krytycznej i wszystkiego, co jest z tym związane.

Natomiast brakowało takiego elementu jak MC, które ujęłoby całościowo kooperację pomiędzy sektorami państwowych rejestrów, finansów, energetyki, transportu, operatorów telekomunikacyjnych i zapewniło wymianę komunikacji pomiędzy tymi sektorami. To w tej chwili się dzieje na bazie Narodowego Centrum Cyberbezpieczeństwa.

Jest tutaj jeszcze jeden ważny element – obywatele. Finalnie okazuje się, że obywatele w domach mają 10 razy więcej komputerów niż znajduje się w całej infrastrukturze krytycznej. Szacunki mówią, że mamy ok. 5 mln komputerów, które są zainstalowane w infrastrukturze krytycznej, wojsku i policji, ale 50 mln komputerów mamy w domach, które stanowią chociażby tablety, telefony. To powoduje, że niezmiernie istotne jest zajęcie się również sprawą zapewnienia bezpiecznego funkcjonowania obywateli w sieci. To też objęliśmy strategią.

Tamten slajd przedstawiał poziom strategiczny. Tutaj mamy poziom operacyjny, czyli poziom bieżącego reagowania, służb, które nadzorują w sposób ciągły cyberprzestrzeń. Narodowy CERT, który znajduje się w Narodowym Centrum Bezpieczeństwa, będzie pełnił rolę huba informacyjnego. Co prawda w opiniach, które się przewijały przez MC, ktoś zasugerował, że narodowe centrum będzie musiało mieć uprawnienia służb specjalnych. Muszę stwierdzić, że niekoniecznie. Centrum funkcjonuje od 4 lipca. Informacje wymienia, ale nie wymienia takich informacji, które upoważniałyby do statusu służb specjalnych. Po prostu zbiera istotne informacje i dystrybuuje je do tych, którzy takich informacji potrzebują. Co jest najważniejsze, to że nasz CERT narodowy funkcjonuje 24 godziny na dobę, 7 dni w tygodniu. Nie tak, jak to bywało w przeszłości, że funkcjonował tylko przez 8 godzin, czyli od 8 do 16.

Sprawa szkoleń jest to kwestia, która pozwala wyegzekwować bezpieczeństwo w cyberprzestrzeni. Szkoleniami chcemy objęcie prokuratorów, sędziów i policjantów, jak również wysokich menedżerów w sektorach gospodarczych, które mają wpływ na funkcjonowanie państwa i na funkcjonowanie gospodarki. Istotni są również projektanci systemów informatycznych.

Dzisiaj życie pokazuje, że informatyków szkolimy w ten sposób, że oni, projektują systemy, myślą tylko i wyłącznie o funkcjonalności, nie myślą o bezpieczeństwie. Dołożenie później bezpieczeństwa do funkcjonalności kosztuje czasami dwukrotnie więcej, niż zaprojektowanie systemu bezpieczeństwa o początku. Dlaczego rozmawiamy już z uczelniami wyższymi, aby w programach nauczania i szkoleń były elementy bezpieczeństwa, na równi z elementami budowy architektury systemu i systemów funkcjonalnych.

Oczywiście, użytkownicy wszystkich kategorii również muszą być szkoleni. Przewidujemy wprowadzenie do programów nauczania takich edukacyjnych elementów dla dzieci w wieku szkolnym, jak również dla wszystkich, którzy eksploatują systemy, czyli w zasadzie dla wszystkich obywateli. Musimy im mówić, jakie zagrożenia w sieci się pojawiają, aby byli tego świadomi.

W zasadzie prace nad strategią zaczęliśmy od początku tego roku. Pierwszym elementem, który pokazał się w kwietniu, były założenia do strategii. Ostatnio zakończyliśmy 7 października konsultacje międzyresortowe i społeczne. W tej chwili opracowujemy ich wyniki. Znajdą się one w kolejnej wersji strategii, uzupełnione o uwagi, które państwo zgłosili. Oczywiście niektóre uwagi się tam nie znajdą, ale my je przyjmujemy.

Już wcześniej mówiłem, że bardzo wiele uwag dotyczy bardzo szczegółowych rozwiązań, których żaden kraj nie umieszcza w strategii. Jeżeli ktoś ma ochotę sprawdzić, to przyniosłem ze sobą cztery strategie, które są dość ogólne. To znaczy, nikt oficjalnie nie pokazuje, co będzie robił. Każdy pokazuje tylko kierunki działania i obszary, w których chce działać. Natomiast szczegóły zostają do planu implementacji strategii. Chcemy zrobić dokładnie tak samo. Szczegóły umieścić w planie wdrożenia strategii.

Jak państwo widzicie, harmonogram jest przedstawiony na slajdzie. Chcielibyśmy w listopadzie, po uzupełnieniu strategii o otrzymane uwagi, przeprowadzić szczeble uzgodnienia na poziomie Komitetu do Spraw Europejskich, Komitetu Rady Ministrów do spraw Cyfryzacji, Komitetu Stałego Rady Ministrów. Pragniemy, aby jeszcze na koniec listopada, może na początku grudnia strategia znalazła się w Radzie Ministrów.

Podsumowując najistotniejsze kwestie. Nie można opóźniać wdrożenia strategii. Obecna sytuacja jest na tyle zła – trzeba wprost powiedzieć – że należy jak najszybciej wiele rzeczy poprawić, trochę na zasadzie gaszenia pożaru. Wdrożenie strategii pomoże nam uzupełnić braki, które znajdują się w wielu systemach, oraz pozwoli przyjąć pewne założenia na przyszłość.

Strategia nie jest czymś, co jest dane raz na zawsze. Można ją modyfikować. Jeśli pojawią się nowe elementy, to będzie można je do niej dołożyć, zmieniając i rozszerzając strategię. Natomiast to, co jest ważne, to że należy ten proces rozpocząć tak szybko, jak tylko będzie to możliwe. Dziękuję bardzo za uwagę.

Przewodniczący poseł Paweł Pudłowski (N):

Tak jak wspominałem, proponuję przedstawić punkty porządku dziennego zbiorczo. Teraz przejdziemy do omówienia projektu ustawy, a potem o wszystkim podyskutujemy.

Dyrektor departamentu MC gen. Włodzimierz Nowak:

Panie przewodniczący, szanowna Komisjo. W związku z powyższym przechodzimy do dalszej części przygotowanej informacji, czyli ustawy o krajowym systemie cyberbezpieczeństwa.

Ustawa jest skorelowana ze strategią. Jaka jest tutaj zależność? Strategia jest wymagana dyrektywą NIS. Przepis w dyrektywnie mówi, że kraje powinny posiadać strategię cyberbezpieczeństwa. Nie czekaliśmy, aż dyrektywa NIS zostanie oficjalnie uchwalona, bo było wiadomo, że nic się w tym względzie nie zmieni. Dlatego strategię zaczęliśmy opracowywać dużo wcześniej, aby nie marnować czasu i nie czekać bezczynnie na ustalenie oficjalnej wersji dyrektywy NIS.

Obowiązuje bardzo wiele aktów prawnych, które dotykają zakresu bezpieczeństwa teleinformatycznego w administracji publicznej. Część z nich pokazałem na slajdach. Nie będę ich omawiał, ponieważ w każdym z tych aktów prawnych jest jakiś drobny element odnoszący się do bezpieczeństwa.

To są również akty prawne, które są związane z bezpieczeństwem teleinformatycznym.

Najważniejsze zalecenie NIK, jakie wynikało z kolejnych kontroli, polecało, aby MC inicjowało i koordynowało działania innych podmiotów w obszarze cyberbezpieczeństwa, w tym budowę ochrony cybernetycznej, szacowanie ryzyk. Jest również ważny element, który jest pokazany jako drugi, w którym najważniejsze organizacje, takie jak Ministerstwo Spraw Wewnętrznych i Administracji, Urząd Komunikacji Elektronicznej, Rządowe Centrum Bezpieczeństwa, Ministerstwo Obrony Narodowej, Komenda Główna Policji, Agencja Bezpieczeństwa Wewnętrznego, Naukowa i Akademicka Sieć Komputerowa powinny mieć przypisane zadania i kompetencje, aby nie ograniczały się tylko do ochrony swoich witryn internetowych. To wszystko ma się znaleźć w naszej ustawie. Nie będę czytał wszystkich zaleceń NIK, bo państwo w większości je znacie.

Kolejnym elementem, który musi się znaleźć w ustawie, są regulacje dyrektywy NIS. Obowiązki nałożone na kraje członkowskie są takie, jak widać, czyli identyfikacja operatorów usług kluczowych, wyznaczanie pojedynczego punktu kontaktowego. Z tym że ten punkt kontaktowy należy rozumieć w sposób specyficzny. Tutaj nie ma intencji i nie ma możliwości, żeby ograniczyć współdziałanie służb specjalnych na poziomie służb specjalnych MON z elementami wojskowymi za granicą. Ten punkt kontaktowy będzie punktem europejskim, do którego będą przychodziły aspekty prawne i aspekty ogólnokrajowe. Nie będą to elementy specjalistyczne, dotyczące służb specjalnych, gdyż one współpracują na własnym poziomie.

W ustawie zaleca się również wyznaczenie CERT dla podmiotów objętych załącznikami, czyli wchodzących w skład infrastruktury krytycznej. Inne działania obejmują udział w pracach grup roboczych, udział w tworzeniu sieci CERT w relacji międzyna-

rodowej i ich współdziałania na poziomie operacyjnym, jak również tworzenie rejestru incydentów dla operatorów usług kluczowych i dostawców usług.

Ustawa o krajowym systemie cyberbezpieczeństwa będzie obejmowała parę głównych elementów. Po pierwsze, chcielibyśmy zacząć od zasad tworzenia dokumentów strategicznych, dotyczących cyberbezpieczeństwa dla Rzeczypospolitej Polskiej, takich jak polityki i strategie. Pragniemy w szczególności określić tempo i sposób wykonywania tych dokumentów.

Po drugie, chcielibyśmy określić organizację krajowego systemu cyberbezpieczeństwa, w tym rolę poszczególnych organów władzy publicznej. Jest to o tyle ważne, że dyrektywa NIS nie obejmuje organów administracji państwowej, a dotyczy tylko i wyłącznie organów biznesowych i usługodawców. Natomiast niepotrzebne jest rozdzielanie tych dwóch aspektów, ponieważ część biznesowa i część państwowa muszą współdziałać. Z tego powodu nie ma potrzeby tworzenia dwóch oddzielnych aktów prawnych. Stąd też regulacja organizacji krajowego systemu jest przewidywana również w ustawie o krajowym systemie cyberbezpieczeństwa.

Z wyprzedzeniem zwróciliśmy się do służb państwowych, żeby zaproponowały nam, co chciałyby, żeby znalazło się w ustawie o krajowym systemie cyberbezpieczeństwa, mając na uwadze fakt, że wciąż będą mogły wykonywać wszystkie uprawnienia zagwarantowane ustawami obecnymi.

Po trzecie, oczywiście implementacja dyrektywy NIS, czyli to obligo, które chcemy wypełnić.

Dodatkowo chcemy w ustawie o krajowym systemie cyberbezpieczeństwa zawrzeć zasady zarządzania cyber incydentami o istotnym skutku zakłócającym. Dzisiaj te zasady nie są jednoznaczne i nie wszystkie służby, nie wszystkie sektory działają w sposób jednoznaczny, tak jak powinny.

Chcemy, aby w ustawie została zawarta również budowa efektywnych programów edukacyjnych i szkoleniowych, poczynając od szkolenia akademickiego, kursów dla menedżerów, szkoleń na poziomie podstawowym dla obywateli, aż do dzieci w wieku szkolnym.

Powinny się tam znaleźć także zasady uczestnictwa ośrodków naukowych w pracach badawczo-rozwojowych i w rozwiązywaniu problemów istotnych z punktu widzenia cyberbezpieczeństwa. W tym celu przewidujemy w strategii tworzenie klastra akademickiego, który będzie stanowił forum wymiany informacji na poziomie uczelnianym. Ważna jest też współpraca w ramach partnerstwa publiczno-prywatnego, które jest nieodzownym elementem, też wymaganym przez Unię Europejską.

Jakie działania w tym celu podjęło MC? Po pierwsze, powołaliśmy grupę roboczą do przygotowania ustawy o krajowym systemie cyberbezpieczeństwa. Grupa pracuje już od dwóch miesięcy. Zorganizowała szereg spotkań z przedstawicielami sektorów. Zaczęliśmy od dyrektywy NIS. Sektory objęte dyrektywą to: sektor energetyczny, bankowy, transportowy. Z ich przedstawicielami rozmawiamy i pytamy, jak z ich punktu widzenia wygląda kwestia cyberbezpieczeństwa, jakie zależności widzą pomiędzy swoimi sektorami a regulacjami dyrektywy.

Sytuacja nie jest zła, ponieważ wiele z tych sektorów już ma wypełnione wymagania zawarte w dyrektywie NIS. Dyrektywa nakłada pewne wymagania, ale u nas w Polsce sektory nie spały. Niektóre same inwestowały w elementy bezpieczeństwa. Skala dodatkowych działań w niektórych sektorach nie będzie zbyt duża.

Planujemy kolejne spotkania z reprezentantami sektorów infrastruktury cyfrowej w celu omówienia punktów wymiany Internetu, usług DNS i innych, które są istotne z punktu widzenia dostarczania usług cyfrowych. W kolejnych krokach będziemy się spotykali z przedstawicielami służb państwowych.

Może przejdę teraz do kolejnego slajdu, żeby pokazać harmonogram pracy. Będzie ona przebiegała w następujący sposób. Listopad i grudzień poświęcimy właśnie na intensywne konsultacje z przedstawicielami służb państwowych i dodatkowe rozmowy z sektorami dostarczającymi usług krytycznych. Po wspominanych dwóch miesiącach chcielibyśmy, aby ustawa nabrała takiego kształtu, aby można było ją w styczniu skierować

na posiedzenie Komitetu Rady Ministrów do spraw Cyfryzacji, w lutym na posiedzenie Komitetu Stałego Rady Ministrów, a w marciu do Rady Ministrów.

Harmonogram jest dosyć napięty, jednakże jest realny. W tej chwili staramy się do końca października nadać ustawie pierwszy kształt. Następnie będziemy już mogli ją dystrybuować i poddawać uzgodnieniom pomiędzy służbami państwowymi a zainteresowanymi sektorami. Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo uprzejmie dziękuję. Czy pani minister chciałaby coś jeszcze dodać, czy możemy otworzyć dyskusję?

Minister cyfryzacji Anna Streżyńska:

Dodam tylko, że dziś ukazał się kolejny raport NIK, który odnosi się do infrastruktury krytycznej. Oczywiście, w większości jest on poświęcony zabezpieczeniu fizycznemu. Jednak podjęte przez nas działania wpisują się generalnie w konieczność zabezpieczenia infrastruktur krytycznych, szczególnie związanej z zaopatrzeniem ludności, ale także z sektorem finansowym oraz z zabezpieczeniem na wypadek różnych innych działań i niebezpieczeństw, w tym także wynikających z niedbalstwa i najbardziej słabego ogniwa w całym łańcuchu wartości, czyli z działania człowieka, jak również z działań celowych.

Już tylko gwoli uświadomienia państwu, że idziemy w pewnym sensie po kolei po poszczególnych elementach systemów informatycznych kraju, nie tylko tych należących do e-administracji, ale także tych, które decydują o codziennym życiu obywateli. Wszędzie jest bardzo dużo do zrobienia. Ten raport NIK także jest bardzo krytyczny.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję pani minister. Bardzo dziękuję panie generale. Otwieram dyskusję. Kto z pań lub panów posłów chciałby zabrać głos? Pan przewodniczący Czarnecki, bardzo proszę.

Poseł Witold Czarnecki (PiS):

Dziękuję bardzo. Podczas poprzedniej kadencji omawialiśmy raport NIK na posiedzeniu Komisji. Rzeczywiście, wtedy pojawił się problem braku koordynacji pomiędzy poszczególnymi sektorami w zakresie bezpieczeństwa. Myślę, że w tej chwili podejmowane przez MC próby wychodzą naprzeciw temu głównemu zarzutowi, a krajowy system cyberbezpieczeństwa w ramach MC będzie głównym koordynatorem cyberbezpieczeństwa krajowego. Sądzę, że taka będzie główna rola systemu, chociaż rozumiem, że wyłączamy sprawy wojskowe, gdyż ten sektor pozostanie uregulowany odrębnie, ponieważ tak musi być. To jest oczywiste.

Jednakże, nie tak dawno zostało powołane Rządowe Centrum Bezpieczeństwa, na czele którego stoi pan Marek Kubiak. Dlatego mam pytanie, jakie relacje będą między tymi podmiotami. W Rządowym Centrum Bezpieczeństwa spraw cyberbezpieczeństwa prawie nie ma. Z tych powodów ważne jest pytanie, jakie będą relacje pomiędzy tymi centrami –Rządowym Centrum Bezpieczeństwa, powołanym przez panią premier Beatę Szydło, i drugim, utworzonym przez MC? Czy między nimi będzie jakaś współpraca?

Na pewno wspomnianą kwestię trzeba uregulować ustawą. Wiem, z rozmów z panem Markiem Kubiakiem, że wygląda na to, że tamto centrum słabo panuje nad sprawami cyberbezpieczeństwa. Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Dziękuję bardzo panie przewodniczący. Jakie są dalsze pytania, komentarze? Jeśli się państwo jeszcze zastanawiacie, to ja mam kilka do pierwszej prezentacji.

Mam pytanie dotyczące slajdu pokazującego, na co będzie położny nacisk. Mam pytanie, czy jest szansa na własny krzem w Polsce? Czy są takie prace w MC, żebyśmy mieli własny krzem?

Mam pytanie o współpracę międzynarodową. Czy są jakieś kraje, z którymi szczególnie współpracujemy? Wydaje się, że Niemcy są przykładem takiego kraju, który jest dobrze zorganizowany pod względem cyberbezpieczeństwa. Jednak, pomimo dość wybi-

jających się ośrodków w Europie w tym obszarze, nie uchronili pani kanclerz przed podsłuchiwaniem przez NSA.

Była też mowa w prezentacji o finansowaniu i o współpracy publiczno-prywatnej. Zawsze niesie to ze sobą jakieś ryzyko. Czy państwo macie już jakąś wizję – w jakim stopniu, w których obszarach będziemy opierali się jako państwo na prywatnych podmiotach?

Mam też pytanie o finansowanie wdrożenia strategii. Czy finansowanie jest już ustalone? Zapamiętałem z raportu NIK bardzo żenującą kwotę, która była dedykowana na kwestię cyberbezpieczeństwa w Polsce. Moje pytanie dotyczy tego, czy dla tak ambitnych planów, które państwo przedstawiliście, będą istniały środki finansowe umożliwiające ich realizację? Na realizację niestety potrzeba pieniędzy.

Nacisk strategii jest położony głównie na infrastrukturę krytyczną, na instytucje rządowe. Pan generał wspomniał o liczbie sprzętu po stronie instytucji i po stronie prywatnej, czy małych i średnich przedsiębiorstw. Stosunek wynosi 1 do 10. Dlatego, z jednej strony, czy położony jest wystarczająco duży nacisk na MŚP, a z drugiej strony, czy nie wymaga się od nich zbytniego zaangażowania? Chodzi o to, jak osiągnąć właściwą proporcję w realizacji strategii, nie narzucając jednocześnie zbyt wysokich dodatkowych kosztów.

W harmonogramie nie ma podanej informacji, dlatego chciałem się zapytać, kiedy projekt ustawy trafi do Sejmu? Widzę ścieżkę dojścia, ale nie ma podanej konkretnej daty, kiedy ustawa pojawi się w Sejmie.

Ostatnie pytanie, które nawiązuje do pytania pana przewodniczącego. Czy rola MC jako jednostki – może nie nadrzędnej, ale takiego *subject matter expert* z prawem weta, np. odnośnie działań MON, MSWiA i ABW, jest potwierdzona przez rząd? Czy jako ekspert w tej dziedzinie macie państwo prawo weto, na przykład w stosunku do wyboru infrastruktury, która może być niespójna? Czy możecie wskazywać obszary, w których wyżej wymienione instytucje powinny realizować określoną procedurę?

Skłamałem mówiąc, że to było ostatnie pytanie, bo mam jeszcze jedno, które mi się nasuwa. Chciałem się odnieść do poziomu ogólności zarysu strategii samej w sobie, ale pan generał odpowiedział, że większość z tych szczegółów – i słusznie chyba – będzie w planie realizacji wdrożenia. Moje pytanie – czy plan realizacji może być przedmiotem utajnionego posiedzenia Komisji? Czy też nie widzicie państwo potrzeby dzielenia się z nami informacjami – w jaki sposób będzie to realizowane? Dziękuję.

Czy nasi goście chcieliby zadać jakieś pytania albo coś skomentować? Jeżeli na tym etapie nie, to poproszę panią minister i pana generała o odpowiedzi. Jeżeli po odpowiedzi nasunęłyby się jakieś komentarze bądź pytania, to zachęcam państwa do zabrania głosu.

Minister cyfryzacji Anna Streżyńska:

Zacznę i spróbuję państwu odpowiedzieć na pytania. W razie czego koledzy mnie uzupełnią.

Jeśli chodzi o pierwsze pytanie dotyczące współpracy międzyresortowej. W szczególności dotyczy to Rządowego Centrum Bezpieczeństwa, które ma bardzo szeroko określony zakres kompetencji. Bezpieczeństwo w tym centrum jest ujęte bardzo uniwersalnie, we wszystkich możliwych aspektach. Myślę, że to właśnie jest w pewnym sensie odpowiedź na pytanie. Z jednej strony jest Rządowe Centrum Bezpieczeństwa, które jest odpowiedzialne za bezpieczeństwo w kraju w ogólnym ujęciu i ma bardzo sprecyzowane zadania.

Z drugiej strony już widzimy po systemie prawnym, że ustawa antyterrorystyczna przyznaje ABW bardzo silne kompetencje, również w zakresie cyberbezpieczeństwa. Jednak są to kompetencje wyspecjalizowane, związane z bezpieczeństwem kraju w kontekście ataków terrorystycznych. Jak się tylko sięgnie głębiej do ustawy, to widać, że są to kompetencje niezwykle mocne, także dotyczące systemów informatycznych, czyli obszaru pozornie przydzielanego właściwości ministra cyfryzacji. Kontekstem, w jakim systemy są weryfikowane i sprawdzana jest ich odporność, wypływa z kontekstu antyterrorystycznego. Zmierza to do tego, żeby systemy informatyczne istotnych infrastruktur krytycznych i organów państwa uczynić bezpiecznymi i odpornymi na każdy atak.

Ministerstwu Cyfryzacji przyznana została rola koordynatora. Czyli w tym momencie nie mamy w żadnej ustawie przyznanych obowiązków i uprawnień kontrolnych czy – jak to pan przewodniczący ujął – prawa weta w stosunku do innych organów. Wydaje się, że z prezentacji wynika wyraźnie, że raczej postrzegamy swoją rolę służebnie, jako dostawcy pewnego rodzaju usług, koncepcji, rozwiązań, procedur, zasad współpracy oraz przepisów dotyczących cyberbezpieczeństwa. Nie mamy, ani intencji posiadania prawa weta, ani potrzeby jego posiadania w stosunku do organów wyspecjalizowanych.

Spójrzmy na strategie innych krajów. Chociażby Estonii czy Niemiec, żeby sięgnąć z jednej strony po najbardziej ucyfryzowanego sąsiada, i z drugiej strony najbliższego, dużego i rzeczywiście bardzo rozwiniętego pod tym względem sąsiada, czyli Niemiec. Te kraje też dzielą obszar zabezpieczenia cyberprzestrzeni na sektor cywilny oraz sektor wojskowy, obronny. Jak słusznie wskazują coraz częściej służby obrony narodowej, cyberprzestrzeń może być przestrzenią wojny i walki. Walka odbywa się pomiędzy różnymi ugrupowaniami, chociażby jakimiś fundamentalistami arabskimi, czy pomiędzy poszczególnymi krajami i narodowościami. Ta sfera nie należy do kompetencji organu cywilnego jakim jest minister cyfryzacji.

Z kolei pilnowanie cyberbezpieczeństwa w sektorach cywilnych, w finansach, w infrastrukturach krytycznych oraz w administracji państwowej, jest typowo cywilnym obszarem. Przestrzega się w całej Europie zasady, żeby ta dziedzina podlegała nadzorowi cywilnego resortu.

Z kim współpracujemy? Między innymi współpracujemy z krajami Unii Europejskiej. Pan dyrektor Nowak jeszcze opowie o swoich działaniach i aktywności, która powoduje, że współpraca jest rozwijana na gruncie europejskim z korzyścią dla wszystkich krajów. Jesteśmy przecież w jednej sieci teleinformatycznej. Co do wspomnianych już na posiedzeniu Niemców: szczególnie współpracują z nami niemieccy partnerzy zajmujący się cyberbezpieczeństwem. Spodziewamy się w najbliższych dniach ich wizyty w Polsce.

Jeśli chodzi o partnerstwo publiczno-prywatne, to trzeba pamiętać, że jak każde partnerstwo wymaga ono współpracy również na gruncie inwestycyjnym, w szczególności w tym sektorze, który tych inwestycji bardzo potrzebuje. Dlatego zarówno my, jako organ wspomagający i MON, jako organ wiodący, zostaliśmy włączeni do strategii odpowiedzialnego rozwoju do działania pod nazwą „Cyberpark Enigma”. W ramach działania, przy pewnym zastrzyku finansowym, mają być realizowane rozwiązania w zakresie cyberbezpieczeństwa. Z jednej strony, pozwolą one nam na podniesienie gotowości ochrony naszej cyberprzestrzeni w sektorze obronnym i w sektorze cywilnym. Z drugiej strony, rozwiną potencjał innowacyjności, a także umożliwią prowadzenie gospodarki innowacyjnej w tym sektorze.

Nie jest wielką tajemnicą, że we wszystkich krajach inwestycje wojska tworzą największe koło zamachowe w nowoczesnych technologiach. W strategii na rzecz odpowiedzialnego rozwoju został dostrzeżony ten wątek i korzyści płynące z wojskowych inwestycji w cyberbezpieczeństwo. Wsparte odpowiednim planem będą realizowane w ramach prac Polskiego Funduszu Rozwojowego.

Prywatne podmioty są częścią cyberprzestrzeni. One potrafią dość dobrze się zabezpieczać. W wielu przypadkach możemy się od nich uczyć. Oczywiście, współpracujemy w pierwszym szeregu z administracją rządową, samorządową, instytucjami badawczymi, na czele oczywiście z naszym NASK. Ważnym partnerem jest również Narodowe Centrum Badań Jądrowych w Świerku, które też ma bardzo rozwinięte kompetencje, jeśli chodzi o cyberbezpieczeństwo. Tutaj poszukujemy najważniejszych dla nas informacji oraz najbardziej istotnego wsparcia.

W tej chwili jesteśmy na etapie budowy kompetencji wiedzy: w jaki sposób dalej budować odporny i bezpieczny system. Jesteśmy bardzo otwarci na podmioty prywatne. Nie jest żadną tajemnicą, że w Narodowym Centrum Cyberbezpieczeństwa funkcjonują operatorzy telekomunikacyjni, sektor finansowy, sektor infrastruktur krytycznych. W jednym *warroomie* spotykamy się głównie wtedy, gdy odbywają się w Polsce jakieś istotne wydarzenia, jak szczyt NATO lub Światowe Dni Młodzieży. Wtedy potrzeba zabezpieczenia sieci jest większa niż normalnie. Tam też następuje wymiana informacji o wszystkich incydentach w sieci, które mogą powodować zagrożenie lub też spowodowały zagrożenie

i trzeba wymienić doświadczenia i informacje, w jaki sposób nie tylko im zapobiegać, ale również naprawić sytuację.

Tam też, opierając się na bezpośrednich doświadczeniach naszego CERT w NASK można wymienić informacje o analizach pochodzących bezpośrednio z sieci i wynikach tych analiz, jakiego rodzaju cyber zagrożenia przeważają, jakiego rodzaju cyber zagrożenia są zarówno u granic Polski, jak i w sieciach krajowych. Mówimy cały czas o zagrożeniach związanych z agresją obcych państw, ale w przeważającym zakresie mamy do czynienia z cyber zagrożeniami pochodzącymi po prostu ze świata przestępczego. Są one skierowane przeciwko firmom, w szczególności przeciwko sektorowi finansowemu, oraz, oczywiście, przeciwko obywatelom, często w postaci drobnych, ale masowych wyłudzeń.

Co do ambitnych planów i kwot na nie przeznaczonych. Tutaj pan przewodniczący dotknął bardzo trudnych zagadnień. Budżet na cyberbezpieczeństwo w MC oczywiście się zwiększył. W poprzednich latach był praktycznie zerowy. Natomiast kilka milionów złotych, którymi dysponujemy, pozwalają nam na to, aby zbudować podstawy bardziej zarządcze i koordynacyjne, niż konkretne rozwiązania techniczne. W planie mamy, oczywiście jako priorytet, i to w naszym budżecie się zmieści, podniesienie bezpieczeństwa systemu rejestrów państwowych. Na wspomniane zadanie mamy pieniądze przyznane specjalną decyzją rządu. Kolejny priorytet to podniesienie bezpieczeństwa całej administracji w postaci rozpoczęcia budowy klastra obejmującego administrację rządową.

Natomiast wręcz nieograniczone potrzeby, które są związane z koniecznością diametralnego podniesienia zdolności obronnych w cyberprzestrzeni przed przestępczością i przed innymi atakami, zamierzamy finansować w pierwszym roku między innymi ze środków badawczych Narodowego Centrum Badań i Rozwoju.

Przygotowujemy duży, wieloletni projekt, który będzie odpowiadał na wiele potrzeb administracji państwowej, w tym również będzie on dotyczył polskiego krzemu, czyli polskiego układu scalonego – o co pytał pan przewodniczący. Również to zagadnienie jest przedmiotem naszych prac, w tej chwili na jeszcze skromnym etapie, w ramach dotacji na 2016 r. przeznaczonej dla Instytutu Łączności. Tam został utworzony zespół specjalistów, którzy orientują się bardzo dobrze w tej tematyce. Nie ukrywam, że naszym marzeniem jest spróbować dotknąć tego tematu i podjąć decyzję o tym, czy inwestować, czy nie inwestować w podobne rozwiązania, na bazie już pewnych doświadczeń opartych na czymś więcej niż marzeniach.

Podobnie, zamierzamy powołać bardzo istotny element zabezpieczania kluczowych dokumentów i systemów informatycznych państwa w postaci wdrożenia norm *Common Criteria*, o czym wielokrotnie wspominała Polska Wytwórnia Papierów Wartościowych. Wydaje mi się, że robiła to również na posiedzeniach Komisji. Zwracając uwagę na to, że wszelkie rozwiązania tego typu certyfikujemy poza granicami kraju: w Niemczech, w Holandii, a także w innych państwach. Nie możemy robić tego u siebie. Od lat mówi się o konieczności zbudowania systemu i zachowania *know-how* dotyczącego naszych kluczowych rozwiązań, związanych z tożsamością cyfrową czy z systemami informatycznymi. Chodzi o zatrzymanie całej wiedzy w Polsce, żeby nigdzie jej nie wynosić i nie dystrybuować poza krajem.

Proces certyfikacji takiego centrum, to są dwa lata ciężkiej pracy, ale jesteśmy do niej gotowi. Koncepcyjnie mamy wszystko opracowane. Jest to, niestety, proces kosztowny, wymagający szeregu praktycznych działań. Stąd też nasze aspiracje, żeby finansowanie podzielić pomiędzy budżet resortu oraz ośrodków naukowych i badawczo-rozwojowych.

Jeśli chodzi o projekt ustawy, to on trafi do Sejmu mniej więcej w kwietniu przyszłego roku. Planujemy w marcu skierować go na posiedzenie rządu. Trzeba liczyć się z tym, że bieg nowej ustawy musi być spokojny. Powinny zostać wyjaśnione dokładnie wszelkie wątpliwości. W marcu zostanie przekazana rządowi, a w kwietniu zapewne skierowana do Sejmu. Oczywiście, przy wszystkich pomyślnych wiatrach. Mam nadzieję, że tak właśnie będzie. Treści ustawy też nie dano raz na zawsze. Będziemy pewnie do niej wielokrotnie wracać i ją doskonalić.

Jeśli chodzi o małe i średnie przedsiębiorstwa oraz ich obciążenie obowiązkami, to w tej kadencji przedsiębiorcy telekomunikacyjni już mocno odczuli obecność państwa. Oczywiście, w kluczowych kwestiach związanych z naszym bezpieczeństwem, niektórzy

dźwigają ciężar interesu publicznego, ale zdarzały się także takie rozwiązania prawne lub ich brak, które zwyczajnie utrudniały inwestycje i obciążały dodatkowymi utrudnieniami. Jako rząd Rzeczypospolitej Polskiej przykładamy bardzo dużą wagę do rozwoju sieci telekomunikacyjnych, w szczególności szerokopasmowych. Nabrały one nie tylko znaczenia cywilizacyjnego dla ludności i dla naszych dzieci, ale przede wszystkim są absolutnie decydującym środkiem rozwoju gospodarczego. Przemysł 4.0 jest oparty w całości na łączności i mobilności. Musimy bardzo mocno w to inwestować. Ostatnią rzeczą, której pragnie minister cyfryzacji, jest generowanie utrudnień czy obciążeń, którym operatorzy nie mogą podołać.

Z kolei względy bezpieczeństwa są kluczowe. Rozwiązania, które muszą objąć 2500 operatorów wpisanych do rejestru przedsiębiorców telekomunikacyjnych, muszą uwzględniać tę kwestię na gruncie ustawy, a później rozporządzeń wykonawczych. Musimy opracować rozwiązania zarówno dla wielkich firm, które stać na bardzo dojrzałe rozwiązania wiążą się z wysokimi kosztami, ale też dla przedsiębiorców, którzy działają w skali jednego bloku, jednej wioski, a czasem jednego osiedla w mieście. Oni też muszą znaleźć w tej ustawie odpowiedź na swoje potrzeby, ponieważ muszą chronić konsumentów, swoich abonentów, przed atakami cyberprzestępców. Nikogo te obowiązki nie ominą. Trzeba będzie bardzo proporcjonalnie dobierać je do skali przedsiębiorstwa.

Plan realizacji jeszcze nie został opracowany. W tej chwili jesteśmy na etapie opracowywania strategii. Jeżeli zostanie przygotowany, to oczywiście są procedury, które umożliwiają komisji sejmowej zapoznanie się z różnymi dokumentami. W moim przekonaniu nie ma przeszkód, aby taki plan – nawet jeżeli będzie zawierał bardzo specyficzne rozwiązania – był co najmniej w części przedstawiony Wysokiej Komisji, ale to już będzie zapewne decyzja Sejmu.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo uprzejmie dziękuję za wyczerpujące odpowiedzi. Czy są jeszcze jakieś pytania lub komentarze? Jeśli nie ma, to bardzo uprzejmie państwu dziękuję. Zamykam dyskusję. Stwierdzam, że porządek dzienny został wyczerpany…

Ekspert Zespołu ds. cyberbezpieczeństwa Polskiego Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej, Bartłomiej Szymczak:

Czy mógłbym zadać parę pytań?

Przewodniczący poseł Paweł Pudłowski (N):

Proszę. Proszę się przedstawić.

Ekspert Zespołu ds. cyberbezpieczeństwa PTPEE, Bartłomiej Szymczak:

Dzień dobry. Bartek Szymczak.

Przewodniczący poseł Paweł Pudłowski (N):

Panie Bartoszu, na przyszłość proszę o lepszy refleks.

Ekspert Zespołu ds. cyberbezpieczeństwa PTPEE, Bartłomiej Szymczak:

Rozumiem. Przepraszam. Reprezentuję Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej, więc patrzę na te kwestie z punktu widzenia operatorów dostarczających energię elektryczną.

Mam kilka pytań. Pierwsze z nich dotyczy celów. Wśród celów strategii wyraźnie podkreśla się bezpieczeństwo obywateli i dostępu do usług elektronicznych, które można też rozumieć jako sklepy elektroniczne, natomiast w samej strategii jest dużo mowy o infrastrukturze krytycznej. Jak państwo planujecie w ustawie uregulować usługi elektroniczne? Jak tę kwestię odróżnić od usług infrastruktury krytycznej? W tym miejscu chcę podkreślić istotę koordynacji wszystkich ustaleń z innymi organami, które regulują działanie infrastruktury krytycznej, jak m.in. Rządowe Centrum Bezpieczeństwa. To jest pierwsze pytanie.

Drugie pytanie dotyczy okresu dostosowania. Ustawa zdefiniuje wymagania, które mogą jednak być trudne w kwestii wdrożenia i czasochłonne. Jaki państwo przewidują okres dostosowania firm do wspomnianych wymagań?

Trzecie pytanie dotyczy finansowania. Jak państwo zamierzają uregulować finansowanie wdrożenia tych wymagań w przedsiębiorstwach? Na ile jest to koordynowane z innymi organami? W przypadku energii elektrycznej jest to prezes Urzędu Regulacji Energetyki oraz minister właściwy do spraw energetyki. Wszystkie inwestycje, jakie przeprowadzają dystrybutorzy energii, muszą być uzgodnione z prezesem URE i przez niego zaakceptowane.

Czwarte pytanie dotyczy CERT-ów sektorowych. W strategii i zapewne w ustawie znajdą się wymagania dotyczące powołania CERT-ów sektorowych. Wyobrażam sobie taki CERT dla energetyki. Jakie miałyby być zasady jego działania? Kto miałby ten podmiot ukonstytuować i powołać? Czy byłoby to ciało państwowe czy prywatne – to też ma związek z kwestiami finansowymi?

Piąte, ostatnie pytanie, dotyczy zasad komunikacji strategii. W założeniach do ustawy jest opisany sposób komunikacji pomiędzy wszystkimi interesariuszami systemu bezpieczeństwa. Jest ich całkiem sporo. Chcę się dowiedzieć, w jaki sposób państwo przewidują płynną komunikację w przypadkach zagrożeń, ataków i sytuacji nagłych, żeby cała konstrukcja nie była tylko elementem raportowania i statystycznego zbierania informacji o atakach, tylko żeby była elementem wspierającym i pomagającym reagować na zagrożenia? Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Czy są jeszcze jakieś pytania bądź komentarze? Jeśli nie ma, to na tym zakończymy. Proszę panią minister bądź pana generała o odpowiedź.

Dyrektor departamentu MC gen. Włodzimierz Nowak:

Postaram się rzeczowo odpowiedzieć na pytania, które dość długo notowaliśmy. Jak zabezpieczyć obywateli i jak ta regulacja będzie wyglądała w ustawie? Jeżeli chodzi o obywateli, to są oni dzisiaj pozostawieni sami sobie. Chcemy wprowadzić takie regulacje, aby dostawca usług internetowych opiekował się obywatelem. Czyli nikogo do niczego nie będziemy zmuszali.

Funkcjonowanie w cyberprzestrzeni jest trochę podobne do jeżdżenia samochodem po drodze. Tu nie może być tak, że jadę po drodze, a z przeciwnej strony jedzie ktoś pijany samochodem bez hamulców i dochodzi do zderzenia czołowego. Jeśli ktoś kompletnie nie dba o swój komputer, nie stosuje dobrych przeglądarek, nie „*upgrade'uje*" systemów antywirusowych, to jest to sytuacja niedopuszczalna. Chcemy wprowadzić taką zasadę, że oczywiście można korzystać z nowych praw i wolności w cyberprzestrzeni, a więc mogę robić, co chcę, ale musi się odbywać to podobnie do jazdy samochodem. Mogę jechać, gdzie chcę pod warunkiem, że jestem trzeźwy, mam prawo jazdy i przestrzegam przepisów ruchu drogowego.

To ma być regulacja, która trochę wyjdzie naprzeciw oczekiwaniu wszystkich, aby inny użytkownik również zachowywał się w cyberprzestrzeni odpowiedzialnie. Czyli, nie będzie dystrybutorem „*exploit'ów*", które zaszyfrują mi dysk. Nie będzie zawirusowywał wszystkich, z którymi się połączy. Każdy z nas będzie musiał wykazać się odpowiedzialnością funkcjonowania w cyberprzestrzeni.

Jednakże, nie każdy się oczywiście na tym zna. Ja mogę zajmować się tym sam, ale jeśli ktoś nie ma takich kompetencji, albo nie chce tego robić sam, to musi mieć szansę wykupienia takiej usługi u operatora czy dostawcy usług internetowych, który za niego będzie o to dbał. To jest jedna rzecz.

Wspomniana kwestia trochę wiąże się z infrastrukturą krytyczną. Zgodnie ze statystyką 15–20% komputerów domowych na świecie jest zainfekowanych. W związku z tym mamy w kraju około 15 mln zainfekowanych komputerów. Teraz sobie wyobraźmy, że wdrażamy szerokie usługi dla społeczeństwa. Łączymy się z rejestrami państwowymi, z urzędami gminy, z urzędami miejskimi i infekujemy systemy państwowe i samorządowe przez swoje komputery. W związku z tym, to stanowi również ochronę infrastruktury krytycznej. Jeżeli pojedynczy użytkownik będzie lepiej zachowywał się w cyberprzestrzeni, to również elementy infrastruktury krytycznej, z którymi będzie się łączył jako obywatel, będą bardziej bezpieczne.

Jeśli chodzi o *vacatio legis*, szczególnie dla regulacji dotyczącej infrastruktury krytycznej, to został on określony w dyrektywie NIS i będzie wynosić 21 miesięcy. Natomiast odnośnie czasu dostosowania do nowych przepisów urzędów państwowych, służb i obywateli, to wszystko to będziemy wypracowywali w drodze negocjacji, ponieważ trzeba wziąć pod uwagę bardzo wiele aspektów. Nie można niczego narzucać, a szczególnie nie można narzucać czegoś, co jest niewykonalne w krótkim czasie. Stąd też okresy *vacatio legis* przy poszczególnych regulacjach będziemy starali się tak dobrać i tak uzgodnić, żeby zmiany były po prostu wykonalne.

Co do powołania CERT-ów narodowych i sektorowych. To jest wymaganie dyrektywy NIS, dotyczące infrastruktury krytycznej i systemów biznesowych. Obowiązek będzie musiał zostać wypełniony w okresie 21 miesięcy, jak już mówiłem.

Wydaje się, że moja wypowiedź wyczerpuje pierwszą część pytań. Natomiast co do zasad komunikacji, to chciałbym, aby omówił je pan dyrektor Januszewicz, który akurat specjalizuje się w tych sprawach. Bardzo proszę.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji Piotr Januszewicz:

Panie przewodniczący, państwo posłowie. Odpowiem na pytanie piąte, dotyczące zasad komunikacji. Uruchomiliśmy w MC projekt, który się nazywa „Zintegrowany system bieżącego zarządzania bezpieczeństwem cyberprzestrzeni”. Program ten ma obejmować podłączenie wszystkich interesariuszy, którzy wchodzą w skład Narodowego Centrum Cyberbezpieczeństwa. Docelowo będą to wszyscy usługodawcy usług kluczowych. Ten system będzie zautomatyzowany. Chodzi o to, żebyśmy czas dystrybucji sygnałów o zagrożeniach zminimalizowali do niezbędnego minimum. W związku z powyższym chcemy wyeliminować proces pracy ludzkiej.

Wszystkie systemy będą połączone ze sobą w jedną, dużą, wspólną sieć wymiany z bardzo dużym elementem nadmiarowym, bo w postaci redundantnych łączy. Łącza będą szyfrowane. Informacja w ramach systemu będzie wymieniana za pomocą międzynarodowego standardu STIX/TAXII. Jeśli w którymś z podmiotów wystąpi atak na infrastrukturę, to urządzenia tam zaimplementowane i systemy detekcyjne wykryją to w sposób zautomatyzowany, na podstawie wcześniej zdefiniowanych reguł. Następnie ta informacja trafi do całej sieci wymiany. Na podsystemie wymiany informacji zostanie z zanonimizowana w taki sposób, aby docierała tylko i wyłącznie do wybranych partnerów – tych, których to interesuje. Jeśli nastąpi np. atak na automatykę przemysłową, to informacja o ataku trafi do tych wszystkich partnerów, którzy korzystają z automatyki przemysłowej. Jeśli będzie to atak na systemy operacyjne firmy X, to trafi to do wszystkich uczestników, bo najprawdopodobniej wszyscy taki system będą mieli u siebie w infrastrukturze.

Zamysł jest też taki, żebyśmy u wszystkich naszych interesariuszy wprowadzili jedną metodykę szacowania ryzyka. Będzie ona polegać na tym, że dokonamy u nich kompozycji systemów teleinformatycznych i sklasyfikujemy każdy element pod względem jego ważności. Jeśli pojawi się sygnatura ataku, to ta sygnatura – w momencie, w którym trafi do odbiorcy – w sposób zautomatyzowany zainicjuje walidację, na ile dany wektor ataku może mieć wpływ na daną instytucję. To będzie odbywało się w sposób zautomatyzowany. W *security operations center* będą mieli wtedy wyświetloną informację, czy należy obawiać się tego wektora ataku w tej instytucji, czy można spokojnie spać, bo ich to w pierwszym stopniu nie dotyczy.

Jeśli chodzi o kolejny element, to jest wymianę informacji z uczestnikami zza granicy. Mamy w planach włączenie naszego Narodowego Centrum Cyberbezpieczeństwa do współpracy międzynarodowej. W związku z powyższym interfejs komunikacji musi być kompatybilny z systemami, które działają za granicą. Będziemy pozyskiwali informacje z Europy, najprawdopodobniej z niektórymi partnerami także ze Stanów Zjednoczonych, w taki sposób, że jeśli się tam zmaterializuje jakieś zagrożenie i będzie znany wektor ataku, to będzie można automatycznie przedystrybuować go do nas, aby nasi partnerzy mogli zostać ostrzeżeni o tym, co się dzieje.

Jeśli chodzi o horyzont czasowy tego działania, to do końca roku chcemy opracować jego koncepcję. Już w tej chwili pani minister wydała decyzję, że NASK będzie opracowywał koncepcję docelową systemu. Zaznaczę jeszcze raz: założenia do koncepcji są opracowane, a NASK w tej chwili już otrzymał je od MC.

W pierwszym kwartale przyszłego roku chcemy zrealizować projekt wykonawczy do całego systemu zintegrowanego. Jeśli się nic nie zmieni, to od pierwszej połowy przyszłego roku chcielibyśmy zacząć implementację systemu dla wszystkich uczestników, którzy będą wpięci do Narodowego Centrum Bezpieczeństwa. To wszystko. Dziękuję.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję za wyczerpujące odpowiedzi. Dziękuję również pani minister i panom za bardzo odpowiedzialne podejście do tej poważnej sprawy.

Myślę, że Komisja trochę się uspokoiła po sesji, która dotyczyła raportu NIK, w którym – co tu dużo mówić – obraz był beznadziejny. Teraz widzimy, że działania zostały podjęte. Jak rozumiem, strategia jest na etapie ukończenia uzgodnień międzyresortowych, tak że czekamy na jej ostateczny efekt. Również do kwietnia czekamy na ustawę, która będzie implementowała dyrektywę NIS. Jak rozumiem, ustawa zostanie wzbogacona o elementy wynikające ze strategii.

Bardzo uprzejmie państwu dziękuję za udział w dzisiejszych obradach. Zamykam dyskusję.

Protokół posiedzenia wraz z załączonym zapisem jego przebiegu będzie do wglądu w sekretariacie Komisji w Kancelarii Sejmu.

Zamykam posiedzenie Komisji.